SANDIA REPORT

SANDNumber Only
Unlimited Release
Printed March 2005

A COMPARISON STUDY OF THE PERFORMANCE ASSESSMENT, PROBABILISTIC RISK ASSESSMENT, AND VULNERABILITY ASSESSMENT METHODOLOGIES

Ann Chang

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

Sandia's nuclear energy risk assessment program has established an international reputation for assessing the safety of nuclear power plants and other critical infrastructures using a Probability Risk Assessment (PRA) approach. Sandia's environmental program has also demonstrated its expertise in performing total system analysis for large-scale geological nuclear waste repositories and established its reputation as a leader in Performance Assessment (PA). In recent years, due to terrorist threats, there is a great need for evaluating the vulnerability of critical targets and assets (Vulnerability Assessment, VA) to support Sandia's commitment to national security. With the goal of better integrating PRA, PA, and VA, this study undertakes to understand the commonalities and differences in the three areas and to identify synergisms and critical research and development (R&D) needs so that focused efforts can be made to maximize the success of this integration.

While significant knowledge and expertise exist at Sandia in these three areas, no single expert has in-depth knowledge in all three areas. Therefore, we conducted a series of expert elicitation sessions to gather information and expert judgments. The results of expert inputs and additional literature study are presented in the report with the author's interpretation, assessment, and conclusions.

This study documents the strengths and weaknesses in these assessment modalities. PRA has broad applications and has demonstrated great value in areas beyond nuclear reactor safety. PA tools are usually designed for specific sites or systems with some common transport and analysis algorithms and applications. In the VA area, evolving and escalating threats to national security continue to require more robust and sophisticated algorithms.

For synergy, a combined suite of PA and PRA tools allows a wider range of applications in several areas. The complexity of security systems and human interactions with them pose challenges. There is an opportunity for the infusion of PA and PRA experience in complex system modeling and integration for VA. In spite of differences in the original intent and applications, the extensive modeling and algorithm development expertise in PRA and PA could benefit the development of more robust VA tools, including uncertainty/sensitivity analysis, multi-target VA, and pathways optimization.

This report is the first step towards exploring integration by expert elicitations. It is hoped the results will facilitate subsequent discussions, identify action areas (e.g., scientific problems and potential customers) and lead to future funding opportunities.

2.0 INTRODUCTION

The goal of this study is to compare (1) performance assessment (PA) tools, developed to describe and predict waste repository performance; (2) probabilistic risk assessment (PRA) tools, developed to characterize and estimate risks from severe accidents at nuclear power plants; and (3) vulnerability assessment (VA) tools, developed to model and predict responder performance and facility damage states when attacked by adversaries.

There are distinctive differences in the problems to which these tools are applied. In terms of methodology, they all use computer codes, perform dynamic system modeling, and are computationally intensive and simulation-based. In terms of sequences of events in the applications, they all can be divided into four phases: initiating event(s) phase, operational phase, progression phase, and consequence phase. PA and PRA tools treat uncertainties more rigorously due to stringent regulatory requirements in capturing the unknown/uncertain nature of problems in several aspects of the models and analyses. VA also expresses results in terms of probability; however, due the nature of the problem (i.e., security vs. safety), certain elements of the VA cannot be realistically assessed. Some VA-associated consequence assessment tools have more capabilities in capturing the probabilistic nature of certain aspects of engineering systems.

The specific objectives of this study are four fold: (1) to compare these tools in their conceptual differences, core methodologies, uncertainty/sensitivity analyses, data collection methods, and error propagation approaches; (2) to identify their strengths and weaknesses; (3) to recognize any synergy among them and potential for integration; and (4) to report areas of future opportunities.

Detailed features of these tools and developmental processes are not the subject of this study. Key references, a brief background, and applications of these tools are provided in the BACKGROUND section.

3.0 BACKGROUND

3.1 Performance Assessment Tools

The PA tools were and are continuing to be developed as part of performance assessments of the Waste Isolation Pilot Plant (WIPP) and Yucca Mountain Project (YMP). The overall responsibilities for the licensing and operating of these facilities include site selection and characterization, experimental studies to understand the interaction of waste and the disposal environment, and transport of radioactive actinides. (WIPP: U.S. DOE, 2004 and Helton et al., 1998; YMP: U.S. DOE, 1998 and U.S. DOE, 2003.)

WIPP is an operational facility for permanent disposal of transuranic waste generated by the defense programs of the United States. Sandia National Laboratories (SNL) was the primary developer of the PA tools for the repository for the 10,000-years regulatory time-frame.

Yucca Mountain, in contrast, is under investigation to be the permanent disposal site of spent nuclear fuel and high-level radioactive waste. SNL is a key participant in the DOE YMP science and regulatory program. SNL's expertise includes performance assessment, numerical modeling, field and laboratory testing, transparency, and quality assurance.

The PA tools dynamically (spatially and temporally) model the gas/brine flows (WIPP) and the underground water flows (YMP) in the repository under both undisturbed or disturbed scenarios. Transport of the radionuclides is modeled initially when the waste drums/packages are naturally degraded. Upon any destructive event(s) over time, the model takes changes in geological formation layers and changes in flow and radionuclide transport in the vicinity of the repository into account. Subsequent flow and radionuclide transport to the assessable environment (WIPP) or the biosphere (YMP) are then computed to estimate radionuclide releases and radiation doses.

3.2 Probabilistic Risk Assessment Tools

PRA tools were developed specifically as part of risk assessment efforts for severe accidents at nuclear power plants. SNL is the lead laboratory in the development of the PRA methods at nuclear power plants. In the NUREG/CR-4551 document series (Gorham et al., 1993), SNL reported an integrated analysis of four accident phases for an overall expression of risk for the U.S. Nuclear Regulatory Commission (NRC). Key references for PRA tools also include NUREG/CR-2300 (1983) and NUREG/CR-6823 (2003). PRA methodology is also applicable to other engineered systems.

The four analysis phases include accident frequency analysis, accident progression analysis, source term analysis, and consequence analysis. Accident frequency analysis determines the likelihood and nature of any initiating event that may or may not result in the onset of the core damage. Accident progression analysis investigates the core damage process both in and outside the reactor vessel and the resultant impact on the containment. Source term analysis estimates the radionuclide release associated with the accident conditions, and consequence analysis calculates the offsite consequences in terms of health effects and financial loss (Gorham et al., 1993).

Both accident frequency and progression analyses are based on extensive use of event and fault trees. Source term and consequence analyses take the result for each accident progression scenario and characterize radionuclide releases through air transport to the environment, including time and length of release, energy release rate, and other factors.

3.3 Vulnerability Assessment Tools

VA tools are developed to identify security vulnerabilities associated with a facility or an operation. They are designed to assess the consequences resulting from adversary attacks to help risk assessors understand the potential risk from various attack scenarios.

SNL performs many security-related studies and analyses to help its customers better manage their security risks. These analyses are done at a systems level and involve differing quantitative and qualitative techniques, depending upon the particular problem being analyzed. Examples of these techniques include process analysis, modeling, simulation, performance evaluation, and cost/benefit analysis.

Most of the VA tools, such as ASSESS and ATLAS, include a description of a facility or an operation under study, a description of the target and threats, a characterization of detection, delay, and response systems being implemented, and adversary attack plans. These tools will perform adversary attack path analysis to identify vulnerabilities associated with facility security systems. They assess system effectiveness presented by probability of interruption by response forces and the probability of neutralization of an adversary. Some of the more advanced VA tools also perform a cost/benefit analysis of a security system upgrade.

4.0 METHODS

Work performed in this study had two phases: a literature review and an expert survey. In the literature review, SAND reports were identified and reviewed. Two comparison charts for methodologies were prepared. The main features/activities for each modeling phase, initiating event(s), progression, source term, and consequence were listed (Table 1). Differences in the overall methodologies were listed (Table 2). The charts gave an overview of the methodologies and facilitated discussions during the survey.

For Phase II of the study, ten experts (developers and expert users) were interviewed. Survey questions asked about strengths and weaknesses for each tool set, their synergy and potential for integration, and future opportunities.

5.0 RESULTS AND DISCUSSIONS

5.1 Comparison Charts

Main features and activities of methodologies by operational phase are presented in Table 1. Some phases of certain tools have more features than others. Key differences and similarities are listed in Table 2. PA tools are primarily used to predict the effects of long-term releases as opposed to the acute and short-term releases predicted by PRA and VA tools. VA tools use likelihood rankings for initiating events, whereas PRA tools use probabilities from historical data. Yucca Mountain PA tools use data from other sources, and WIPP PA tools use a Poisson distribution with assumed values for the parameters. VA applications frequently have humans in the loop; PRA applications have limited human interactions. PA applications naturally assume no human interactions after the closure.

5.2 Conceptual Differences and Regulatory Requirements

The conceptual structure of the analysis will determine how each tool is applied. PA tools emphasize the long-term (100,000 to 1,000,000 years) performance of the repository, and they typically average over all possible future event scenarios for estimation of releases. PRA and VA tools, on the other hand, are primarily incident/accident driven and are used to report outcomes of acute scenarios. The conceptual structure of the PA derives from regulatory requirements imposed on the facility. PA and PRA tools have rigorous treatment of uncertainties.

For WIPP PA, three requirements of 40 CFR 194 (U.S. EPA 1996) were addressed: (1) a probabilistic characterization of the likelihood of future events; (2) a procedure for describing the release mechanisms and estimating the radionuclide releases to the accessible environment; and (3) a probabilistic characterization of the uncertainty in the parameters based on experimental data and expert panels. Cumulative releases of radionuclides to the accessible environment are required not to exceed some boundary lines (40 CFR 191; U.S. EPA, 1985).

For Yucca Mountain PA, 10 CFR 63 requires that the performance assessment estimate the dose required by a reasonably maximally exposed individual, including the associated uncertainties, as a result of releases caused by all significant features, events, processes, and sequences of events and processes, weighted by their probability of occurrence (U.S. DOE, 2003).

Safety assessment for reactor site selection required by the NRC (10 CFR 100) includes an assumed 25 rem exposure at all times. For severe accidents modeled by PRA, it is not possible to impose exposure requirements. Nonetheless, given an accident scenario, PRA tools are required to describe physical phenomena and the use of probabilistic techniques to characterize uncertainties, use of expert panels to develop distributions for important phenomenological issues, and automation of the overall analysis (Gorham et al., 1993).

VA tools estimate adverse effects of attacks by adversaries. They are all scenario-driven and have no regulatory requirements.

5.3 Modeling of Transport

PA involves modeling and simulation of a source (e.g., radionuclides) transporting through physical media (e.g., vadoze zone, groundwater, etc.) and then predicting the dispersion of the source in the media as a function of time. Transport mechanism through media of interest becomes a centerpiece of the modeling effort and has a direct effect on the validity of the assessment. WIPP PA uses a two-dimensional (2-D) geometry for computation to solve a system of differential equations over time. Yucca Mountain PA is abstraction-based, requiring look-up tables.

PA and PRA, when compared as used in assessing reactor safety, are similar in that PRA is also modeling failures transporting through an engineered reactor system and predicting the final failure and consequence resulting from such failure propagation. Although PRA can be viewed having such a conceptual similarity with PA, the mathematical framework and formulations could look very different from those used in a PA. PRA starts with event-tree or fault-tree analysis, which has different mathematical forms from transport models used in PAs. However, the consequence assessment part of PRA includes transport of a source (e.g., radionuclides) through air and prediction of the dispersal of the source in the air medium as a function of time, which is the same concept as the PA transport modeling. Due to the large number of sequences or paths in the fault/event trees, grouping or binning is common in the PRA analysis during the three interfaces of the four analysis phases (including accident frequency analysis, accident progression analysis, source term analysis, and consequence analysis). For example, many paths in the accident progression analysis are grouped into bins for source term analysis, where each bin defines a similar set of initial and boundary conditions.

VA models the transport of a source (for this purpose, an intrusion) through the security system associated with a facility or an operation. It also assesses the progression of adversary actions (transport through the system) in the security system as a function of time. Detection, delay, and response systems are engineered “physical media” (barriers) designed to slow down the progression of adversary actions. The mathematical expression and model formulation of VA look similar to those used in PRA. An essential part of VA is to develop Adversary Sequence Diagrams (ASD) to describe how an intrusion would occur and penetrate through the security system and its likelihood of being detected, delayed, and stopped. Since security vulnerability is identified by analyzing each potential path into the target area, the term “pathway analysis” is often used, and pathway analysis is similar to event-tree evaluation.

5.4 Initiating Events and Uncertainty Analysis

Initiating/destructive events are events that could initiate a release, an accident, or damage. For WIPP PA, such events are drilling and mining. For Yucca Mountain PA, such events are the formation of a volcano, an earthquake, or nuclear criticality. WIPP PA applications in general characterize these destructive events using a Poisson distribution with assumed parameter values, while PA applications for YMP are based on available data from other outside sources. PRA tools group initiating events in categories of either internal or external events. This grouping is based on past experience in operation. External events are largely initiators that occur outside the plant, including earthquakes, hurricanes, and floods, but can also include fires within the plant. Internal events include transients, loss-of-coolant accidents, and steam generator tube ruptures, but can also include losses of offsite power. Mean frequencies are estimated using historic data (Poloski et al., 1999). Destructive events for VA could be theft, destruction of operation, and espionage. Because it is difficult to capture uncertainty associated with human behaviors, likelihood rankings are often used.

Both stochastic uncertainty (aleatory) and subjective uncertainty (epistemic) are addressed in PA and PRA. Stochastic uncertainty arises from many possible disruptions that could occur over time. Subjective uncertainty arises from imprecision in the parameters of the equations in the models. VA tools, on the other hand, use mostly likelihood rankings based on expert judgment and patterns of real attacks. Uncertainties in PA, PRA, and VA are normally expressed as distributions of defined parameters based on experimental data, performance testing, or expert judgment. The process includes identification of uncertain parameters, their ranges, and distributions. The process and model input used have to be technically defensible in order to appropriately represent uncertainty in the model predictions. Uncertainty analysis includes the following steps: random sampling, iterative model development, and sensitivity analysis. Monte Carlo sampling (or more efficient sampling techniques, such as Latin Hypercube Sampling [LHS]) is often used to draw samples from distributions and compute predictions with the proper uncertainty reflected. Development of models involves an initial broader information base, then repetitive testing, data collection, and model refinement and validation. Sensitivity analysis is part of this model-building process and is used to identify critical areas for iterative improvement. Estimates of uncertainty distributions for key modeling parameters become a critical task and could be both time and resource consuming. Sensitivity analysis, data collection processes, error propagation approaches, and software codes are discussed in the following sections.

5.5 Sensitivity Analysis and Data Collection Methods

The purpose of sensitivity analysis is to reveal the relationships between model inputs and model predictions and, more importantly, to uncover model parameters that would have more impact on the outcome of the predictions. The "list" of key variables is not immediately finalized until confidence in the system is gained and performance insights are obtained. Confidence is gained by using an iterative process of conducting experiments on various aspects of the system where knowledge is lacking, rigorous data collection/validation and analysis, and/or structured expert elicitations. Sensitivity analysis is used as a tool of key area identification and prioritization along with these data collection and learning steps to help achieve the goal of complex system learning.

Sensitivity analysis techniques such as scatter plots, linear regression, stepwise regression, correlation and partial correlation, and rank transformation have been established and published by Helton (1993). Other techniques include entropy-based analysis and classification-tree-based analysis (U.S. DOE, 2003). These analyses use data from all available sources. Observational data from operations, incident/accident reports, and testing (when actual experiments are feasible) are utilized. When observational data is not available, the expert judgment process is designed to obtain subjective estimates of the unknown physical quantities and frequencies. Principles and guidance have been carefully established and extensively exercised through the development of the tools. Sensitivity analysis plays a significant role in the development of PA and PRA models. It plays a lesser role in VA development, but that may change in the future when VA tools have to capture the characteristics of a complicated engineering system designed to meet new escalating threats.

5.6 Error Propagation Approaches and Model Outcomes

Both PA and PRA use random sampling and LHS schemes. VA, if used, adopts mostly the random sampling schemes. In random sampling, there is no assurance that points will be sampled from any given subregion of the space, especially if a limited number of samples are taken. Also, it is possible for an inefficient sampling of the space to occur if several sampled values fall very close together.

LHS ensures the full coverage of the range of each variable. Random sampling is the preferred technique when sufficiently large samples are possible because it is easy to implement, easy to explain, and provides unbiased estimates. LHS is used when large samples are not computationally practicable (Helton et al., 1996).

In WIPP PA simulations, for example, a sample from the distributions of the model input/parameters is first taken as the outer loop. It is followed by a second sample of one future (over time) with its associated series of destructive events as the inner loop. The results of this performance assessment are computed. The inner loop is repeated the desired number of times and an average of all possible futures is computed. The outer loop is then repeated to compute releases for subsequent simulation for the desired number of times. Variations specified in the parameters and destructive events are propagated throughout the computations and reflected in the model output. This error propagation concept is similar for PA, PRA, and VA, although the usage for VA is not across the board and is not as extensive.

For PA and PRA, model outcomes are primarily presented as the complementary cumulative distribution functions (CCDF) or the exceedance frequency curve. It is the probability or the frequency of model predictions that are actually exceeding the regulatory boundary line or beyond certain allowable outcome. CCDFs are the primary outcome for WIPP PA. Yucca Mountain PA allows CCDFs under three weather conditions. It also computes ingestion dose and inhalation dose as well as total dose and health effects. PRA allows weather sampling and computes inhalation dose, ingestion doses, early and delayed health effects, loss of habitability of areas, and economic losses. The consequence assessment part of VA could have various different representations such as the number of deaths or injuries, the economic cost, operator’s cost, damage level, recovery time, cascading (domino) effects, and psychological effects.

5.7 Software/Codes

PA software for both WIPP and YMP includes a suite of computer codes that are interconnected (U.S. DOE, 1998 and U.S. DOE, 2003). The PRA codes SAPHIRE, EVNTRE, MELCOR, and MACCS2/WIN MACCS are executed either separately for each analysis phase (initiating event(s) phase, operational phase, progression phase, and consequence phase) or in sequence as an integrated study. The VA codes ASSESS, ATLAS, and EASI evaluate the vulnerability of a facility or an operation. EASI is the simplest version, and ATLAS is the upgrade of ASSESS. JCATS is a combat simulation tool for the evaluation of protective force effectiveness in responding to an adversary attack. RAM-D and RAM-W are risk assessment methodologies developed to assess the likelihood of a failure and the associated consequences. Other codes such as ERAD and CTH are often used to assess consequences and damages resulting from an attack. They were developed independently and not intended for integration.

5.8 Strengths

Risk assessment tools have served their purposes well. In the PA area, the WIPP performance assessment standards have become internationally accepted and led to the opening of the waste repository. PRA methodologies have been extensively reviewed by peers, industry groups, and regulatory agencies (e.g., the American Nuclear Society, the Advisory Committee on Reactor Safeguards) and have led to an increased awareness in the nuclear power industry of the need to consider uncertainties in risk studies. Vulnerability assessments and their ability to develop countermeasures against adversary threats in buildings and facilities have proven essential for homeland security concerns.

Probability assessments have found significant applications in WIPP and YMP geological repositories. Detailed site characterization data provide a foundation for the PA models developed for these sites. Lessons learned from early WIPP application, the modular nature of more recent PA tools, and the ease of adding other process models and codes have improved the effectiveness of PA tools. In addition, recent PA tools are more flexible in allowing changes and thus the codes have more universal acceptance. Codes for Yucca Mountain PA have shell capabilities and are more user-friendly. WIPP PA tools are considered freeware and are written according to software requirements for the nuclear industry.

Current PRA tools have been well researched and established; they can be used for evaluation of other engineered systems. Through fault/event tree and other analyses, PRA tools provide a logical framework for identifying undesirable safety outcomes. Successes have also been demonstrated for other applications, including nuclear weapon systems and aviation risk assessment. Continued growth in that area and other areas such as satellites, spacecraft, and communications holds great potential.

The framework for designing VA tools is the Design and Evaluation Process Analysis process developed at SNL and based on years of experience in security systems and technology. This process describes not only how to design an effective Physical Protection System (PPS), but uses an iterative process to evaluate the design and continue to improve the PPS.

5.9 Weaknesses

A major limitation of PA tools is the uncertainty resulting from using physical and mathematical formulations to capture the nature of environmental behavior. Although the goal of scientific theories, data collection, and mathematical modeling is to reduce modeling uncertainty, environmental variables are very difficult to predict and capture accurately, especially over a long time period (e.g., 10,000 years). Scenario predictions also have limitations because of the uncertainty in future site protection, characteristics, development, human living styles, habits, and infrastructures. In some cases, 1-D or 2-D simulation of the 3-D source transport in environmental media also pose some limitations.

Some complicated codes, such as the WIPP PA tools, require a lot of code-specific expertise to use the model. The learning curve for new operators can be significant. Some of the PA tool modules for YMP assessment do not run dynamically and need to be run in steps. A large number of pre-generated models would be required to accommodate possible future design changes. It is impossible to foresee all future changes. The complexity of the model (e.g., over 200 uncertainty parameters, the number of pre-generated models) also makes it difficult to maintain and ensure quality control of code modification.

Although PRA is a very powerful tool for characterizing the probability in each failure mode and propagating the errors for an end assessment, the lack of data, specification, and/or computation resources force the use of binning of failure modes in risk assessment for nuclear industry applications. A potential drawback of binning is the loss of information, which could lead to a biased assessment and missed insights if key mechanistic paths were binned. To overcome binning, an increase in computing power would be required.

Existing VA tools have limitations in assessing attack scenarios to multiple targets. Although single runs can be combined, the dynamics of attack scenarios on multiple targets may not be captured accurately. Attack scenario inputs (adversary motivation, capability, tactics, etc.) have a direct impact on the assessment results. It is a challenge to capture representative and bounding conditions for adversary attacks with realistic assessment of ever-changing threats. Uncertainty associated with human behaviors both from adversary and response forces and their interactions with engineering systems are also difficult to represent accurately.

5.10 Future Opportunities for PA, PRA, and VA

PA tools have been well developed for several large-scale applications in the U.S. and may have an international market. It should be noted that the application of PA is not limited to large-scale geological repositories for nuclear wastes. Applications in the mining industry, for example, include evaluation of mine closure options, mine water management, and long-term strategic planning. PA codes have applications in the water resource area in predicting extreme hydrologic events such as floods and droughts, describing aquifer remediation and restoration undertakings, and developing erosion and sediment dynamics models. PA codes modeling environmental pollutants contain transport models of groundwater contamination and management models for groundwater remediation from agricultural practices and other hazardous wastes. Many of these efforts require computer models such as performance assessment models, geographic information systems, decision support systems, and multimedia computing environments. Many of these models require stochastic and uncertainty analysis.

Generic PRA tools, not necessarily specific to nuclear power plant applications, have been well developed and can be used for evaluation of other engineered systems. PRA tools include fault-tree and event-tree analyses to describe the reliability and safety of complex system models. Used with sensitivity analysis of preliminary performance data (e.g., determining which event would contribute to more overall system safety), key events/failure modes of the system can be initially identified. When more performance data of these events is collected, either raw data or expert-based, the next iteration of the sensitivity analysis can be performed to identify or update the set of key events. During this iterative process, insights into a complex system can be gradually revealed.

Life-cycle analysis using operational data allowing time-dependent predictions of aging effects, performance trends, and instantaneous risks are other capabilities available through use of PRA tools. Specific hazard assessment can then be carried out/estimated for preventive measures and actions. Additional PRA tools include time-series analysis, reliability analysis, quality control methods, geostatistics, experimental design, and sampling methods. Any of these tools, or combinations of them, can be used to describe specific system problems. Successes have been demonstrated for the areas of nuclear weapons and aviation risk assessment. Industry and government customers such as the FAA, NASA, U. S. Air force, NAVAIR, and Lockheed Martin will allow these codes to gain further application.

VA tools have existed for many years and are receiving more attention recently due to the emphasis on homeland security and counterterrorist measures. A major difference between VA and PA/PRA is that vulnerability assessments take into consideration human action as a main parameter. The difference between security (VA) and safety (PA/PRA) applications also separate them. For example, VA deals with human intent and behaviors and it is very difficult (or impossible) to estimate the likelihood of attack while safety-related initiating events can normally be represented statistically based on historical data. In the field of security, the predictability of historical data is rather limited. Traditionally, security assessment relies heavily on expert evaluation, judgment, and field exercises. However, due to the increasing threats and escalating costs for security forces, there is a growing need to deploy advanced technology and systems to assist security forces in defending their sites and operations. As a result, the complexity of security systems intensifies and the assessment of system vulnerability becomes less obvious and requires more computer tools to assess the system effectiveness by considering all the interconnectivity and interactions. The need for developing advanced VA tools to perform accurate and sophisticated analysis for high-valued sites and operations continues to grow.

5.11 Synergy between PA and PRA

PA tools coupled with PRA capabilities allow a broader range of applications. GoldSim Technology Group, a commercial software, training, and expert consulting company and the provider of the primary simulator for the PA at YMP, recently introduced its reliability module for PRA. In a recent article [ref GoldSim PRA paper], the GoldSim model was compared to the standard NASA PRA approach. Differences between the two in identification of initiating events, structuring scenarios and logic modeling, fault tree and event tree, and uncertainty analysis were discussed. With its suite of simulation modules, the GoldSim Technology Group addresses challenges in radioactive waste, mining, water supply and treatment, oil and gas, and other areas.

In developing PA models for geological repositories for nuclear wastes, the mining industry, water resource areas, and environmental pollutants and contaminants transport, the following modeling steps are taken: data collection, model assumptions, iterative model building, and diagnostics and validation. Environmental variables of PA models of large-scale repositories are very difficult to predict and quantify accurately, especially over a long time period. One of the reasons for this difficulty is that full-scale environmental testing over the desired time-frame is impossible; thus, the model diagnostics and validation process is also not possible. This is not the case for many of the applications discussed above on smaller-scale (both in scope and in time) applications where testing data is possible. For such applications, models can be validated using generic PRA tools. Geographic information systems (GIS) software and geostatistics also provide powerful tools for the description of spatial patterns and spatial uncertainties of contaminated sites.

5.12 Synergy between PA and VA

Sensitivity analysis methodology and software have been well developed for PA applications. Such analysis can identify a set of model parameters whose changes would have a relatively large impact on model predictions so that research effort can be focused on reducing overall model uncertainty. This type of analysis could potentially be coupled with VA models to evaluate which system parameter in a security system would most impact the detection, delay, and response. For example, the probability of interruption, which is a key component in determining overall system effectiveness, is the cumulative probability of detection up the critical detection point defined based on an attack path. Sensitivity analysis may be used to identify the most sensitive detection systems based on individual system probabilities.

PA tools describe agent transport, hydrology, and earth/geologic changes. To predict the consequence of a sabotage event (e.g., dispersal of chemicals through water or other media), PA expertise and modeling experience could also be potentially helpful in assessing the impact, for example, of contaminated reservoirs/dams or distribution infrastructure. However, it should be noted that the initial transport and dispersal resulting from a sabotage event is most like to occur quickly to cause the maximum impact, which is somewhat different from the time-frame of a typical PA.

There are also questions from PA experts on whether statistical methods using probability distribution can be used to assess the likelihood of attack. VA experts question whether it may be difficult to apply statistical methods to predict adversary behaviors and their selection of attack targets and tactics. Likelihood of attack, target selection, and attack scenarios have thus far been based mostly on the analysis of terrorist behaviors, attack histories, and red-team judgment. Use of statistical methods or distributions has not been proven valid.

5.13 Synergy between PRA and VA

The discussion below focuses on the synergy between PRA and VA tools for vulnerability assessment of nuclear power plants. The need for improvement in these kinds of applications is identified. Many of the recommendations relate to software improvement.

5.13.1 Spatially Informed Models vs. Random Effects Models

Traditional probabilistic risk assessment of nuclear power plants considers that accident-initiating events occur in a random manner (e.g., power pump failure). In an attack situation, the assumption of a random event is not valid because adversaries will study the system and select the weak link or specific targets based on the situation. In such a case, the logic model with event trees and fault trees could become extensive and harder to manage because, for example, there could be a large number of electrical wires connected to the power pump at various switches and distribution centers that may cause the power pump to fail. Therefore, earlier codes written for random effects modeling require improvement to meet such needs or the random effect modeling should be supplemented or replaced by a spatially informed model.

5.13.2 Success Paths/Target Sets

PRA tools were initially designed to describe failures and accidents. To protect critical targets and ensure absolute safety, success paths and target sets need to be identified. Current PRA codes are cumbersome for these kinds of applications and need to be improved or modified to be effective. One approach is to couple PRA capability with VA tools since VA tools are designed to identify success (vulnerable) paths for selected targets.

5.13.3 Target-Rich Environments and Multiple Target Attacks

Current VA tools have the capability to perform single or multiple path analyses for the same target. For a typical nuclear power plant, several potential targets may exist and could be attacked at the same time. Codes for multiple target attacks are not currently available.

5.13.4 Efficiency of Computer Codes

Due to the added complexity for vulnerability assessment, existing codes for PRA analysis would benefit by taking advantage of modern computer hardware and software technology, such as parallel processing, for greater efficiency.

5.13.5 Structural Response of Facility

Building structural response to extensive external attacks (e.g., from an aircraft) is not well understood. The need to continue basic science in structure and fire is apparent.

5.13.6 Other Potential Areas

Synergy between PRA and VA tools for vulnerability assessment of other industries, including communications, power grid, food supply, and critical infrastructures, is worth reiterating. Existing tools plus expert domain knowledge in these areas present new opportunities.

5.14 Human Capital and Suites of Tools

In addition to modern science and computer technology, human capital is a critical element in solving these complex problems. Experience and expertise is needed in the areas of treatment of uncertainties, advanced programming, simulation and sampling routines, fault/event tree analysis, and numerically solving series differential equations. Development of the assessment process began with data and questions from multiple resources. Researchers began with a large information base, then formulated this information into the conceptualization pieces to show how various processes work, which will be further developed into a more compact and usable form of the system description. A tremendous amount of experience was accumulated to go through this iterative screening process methodically and collaboratively to identify the next set of key areas or "abstractions" to eventually arrive at the final presentation of the model.

The combination of experience, tools, and reputation means potential for these codes. Teaming with experts in other domains would give even greater flexibility and opportunities to develop suites of tools to support wider applications, including environmental systems modeling, engineered systems modeling, critical infrastructure modeling, and vulnerability assessment modeling.

	Initiating Events	Operational Phase	Progression Phase	Source Term Description	Release to the Environment
PA-WIPP	drilling, mining	material degradation, transport pathways, natural system response, engineered system response	degradation, direct releases due to cuttings, cavings, spallings, and direct brine release long-term releases due to groundwater transport in culebra and salado	radionuclide type and radionuclide concentration	CCDFs
PA-YM	volcanism, seismic activity, nuclear criticality	material degradation, transport pathways, natural system response, engineered system response	degradation, direct release scenarios, enhanced source term scenarios, indirect volcanic effect scenarios, rockfall scenarios, in- and out-of package criticality scenarios	radionuclide type and radionuclide concentration	biosphere dose conversion factors, ingestion dose, inhalation dose, and CCDFs allowing 3 weather conditions
PRA	transients, loss of coolant accidents, steam generator tube ruptures, loss of offsite power	systemic event trees and fault trees, sets of component failures to core damage, frequencies of accident sequences	event trees, events in the reactor vessel and the containment, physical phenomena affecting the progression	radionuclide class, timing of release, energy release rate, release fraction	inhalation and ingestion doses, early and delayed health effects, loss of habitability of areas, economic losses, CCDFs allowing weather sampling
	earthquakes, hurricanes, floods, fires				
VA	theft, damage (insiders & outsiders)	single path analysis, multiple path analysis, simulations, tactics/strategies, resources, response time	event trees, fault trees, (e.g., water supply system --dam damage), water channel wiped out, contaminated reservoir, purification facility	radionuclide type, radionuclide concentration (code-dependent)	human injuries/deaths, structure damages, economic impacts

Table 1. Features and Activities of Each Methodology by Operational Phase

PA	PRA	VA
geology, hydrology, geochemistry, geophysics	air dispersion, meteorology, nuclear power plant operation, core damage physics	consequence in all media
releases/10,000 yrs (primarily) or acute	releases/annual or acute	acute (releases or damage/intrusion)
releases (CCDFs), concentration, doses, and health effects	releases (CCDFs), inhalation and ingestion doses, health effects, loss of habitability, economic losses	code-dependent
releases are averaged over initiating events	releases are initiating-event specific	scenario-based
random and LHS sampling	random and LHS sampling	random
long-term predictions	acute phases	acute phases
local software (WIPP) local software + GoldSim (YM)	local software based on similar framework	common software and local modifications
light use of formal fault tree/event tree	heavily uses fault tree and event tree analyses	more pathway analysis (event tree concept)
initiating events are assumed to have a Poisson distribution (WIPP) or are based on other available data sources (YM)	probabilities of initiating events are estimated based on operational data	likelihoods category at most
no human interactions after initiating event(s)	limited human interactions	frequent human interactions
assuming no initiating events until after the closure	initiating events during operation	emphasize operational phase
spatial and temporal	spatial and temporal	temporal sequence in an attack
stochastic and subjective uncertainties	stochastic and subjective uncertainties	likelihoods and rankings

Table 2. Differences/Similarities in Modeling Features and Emphases
(exceptions exist in some areas)

6.0 Acknowledgements

The author would like to acknowledge the contributions from the experts who have provided input to this study. Their names are listed below. In addition, management support from Marianne Walck, Mark Allen, and Kathryn Knowles is greatly appreciated.

Experts who contributed:
Nate Bixler
Sean Dunagan
Julie Gregory
Cliff Hansen
Cliff Ho
Mike Itamura
Kathryn Knowles
Patrick Mattie
Lee Shyr
Josh Stein
Donnie Whitehead
Tim Wheeler

7.0 References

Atwood, C. L., LaChance, J. L., Martz, H. F., Anderson, D. J., Englehardt, M., Whitehead, D., and Wheeler, T. 2003. "Handbook of Parameter Estimation for Probabilistic Risk Assessment." NUREG/CR-6823, SAND2006-404840483348P.

Gorham, E. D., Breeding, R. J., Helton, J. C., Brown, T. D., Murfin, W. B., Harper, F. T., and Hora, S. C. 1993. "Evaluation of Severe Accident Risks: Methodology for the Containment, Source Term, Consequence, and Risk Integration Analyses." NUREG/CR-4551, SAND86-1309, Vol. 1, Rev. 1.

Helton, J. C. 1993. "Uncertainty and Sensitivity Analysis Techniques for Use in Performance Assessment for Radioactive Waste Disposal." *Reliability Engineering and System Safety*. **42**(2-3):327-367.

Helton, J. C., Bean, J. E., Berglund, J. W., Davis, F. J., Economy, K., Garner, J. W., Johnson, J. D., MacKinnon, R. J., Miller, J., O'Brien, D. G., Ramsey, J. L., Schreiber, J. D., Shinta, A., Smith, L. N., Stoelzel, D. M., Stockman, C., and Vaughn, P. 1998. "Uncertainty and Sensitivity Analysis Results Obtained in the 1996 Performance Assessment for the Waste Isolation Pilot Plant." Sandia National Laboratories. SAND98-0365.

Poloski, J. P., Marksberry, D. G., Atwood, C. L., and Galyean, W. J. 1999. "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995." NUREG/CR-5750, INEEL/EXT-98-00401.

U.S. Department of Energy. 1998. “Viability Assessment of a Repository at Yucca Mountain – Total System Performance Assessment.” DOE/RW-0508, Vol. 3.

U.S. Department of Energy. 2003. “Total System Performance Assessment – License Application, Methods and Approach.” TDR-WIS-PA-000006.

U.S. Department of Energy. 2004. 40 CFR Part 191: “Compliance Recertification Application for the Waste Isolation Pilot.” DOE/WIPP 2004-3231, U.S. Department of Energy Waste Isolation Pilot Plant, Carlsbad Field Office, Carlsbad, NM.

U.S. Environmental Protection Agency. 1985. 40 CFR 191: “Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Waste; Final Rule.” Federal Register **50**:38066-38089.

U.S. Environmental Protection Agency. 1996. 40 CFR Part 194: “Criteria for the Certification and Re-Certification of the Waste Isolation Pilot Plant’s Compliance with the 40 CFR Part 191 Disposal Regulations; Final Rule.” Federal Register **61**(28):5242-5243.

U.S. Nuclear Regulatory Commission. 1983. “PRA Procedure Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants.” NUREG/CR-2300, DE84 900179.